



## People-Centric Data Loss Protection to track and remove at-risk sensitive data

### The Challenge:

- Defend against sensitive banking information leakage from Slack & Google Drive
- Secure company's brand from accidental or intentional data loss
- Increase employee awareness from phishing & other unsafe data sharing practices

### The Solution:

- Polymer DLP for Slack
- Polymer DLP for Google Drive

### The Results:

- Real time visibility into sensitive data traffic
- Blocked virtually all sensitive files to be shared with unauthorized persons
- Removed over 97% of all sensitive data elements shared in public chats in real time
- Suspicious activity monitoring surfaced potential internal threats

## The Challenge

Routefusion is a high growth cross-border payment SaaS platform used by banks. The KYC and other bank requirements puts it in the forefront of collecting sensitive information at the time of account opening and during course of business. Working with some of the most strict data privacy laws and international regulations, Routefusion needed a complete data loss protection solution.

When head of operations, Michael Cramer joined Routefusion, he was charged to build a scalable operation that can handle 500%+ growth without compromising on PCI compliance, security, PII/PHI privacy.

“Routefusion works with highly regulated banks with strict privacy laws-Polymer was able to make our Slack & Google Drive PCI compliant very fast”

He was charged to look for solutions and practices that did not get the way of how work was happening while also instilling a privacy-first culture within the firm and its partners. After evaluation several vendors, he decided to hold a proof-of-concept (POC) to assess the efficacy of Polymer.

“Polymer just worked out of the box. Minimal tweaking of rules with great support was done within 2-3 sessions”

The trickiest part of this problem was to secure Slack Connect channels with external parties without undue burden on how actual transactions were occurring.



## The Solution

Sensitive Data Loss Protection achieved for Routefusion

Routefusion founded its solution Polymer DLP and its unique people-centric approach to security. With Polymer DLP for Slack and Google Drive in place, the first step was to get a sense of the amount of sensitive data traffic. With the 'Tracking Only Mode' within Polymer, all events within Slack and Google Drive were monitored and logged.

"We were able to immediately get a list of public file links on Google Drive and who has access to what"

Next, the team focused on describing the permission levels of the firm by applying entity level permissions throughout the organization. This step took 25 minutes and by the end of it the User level reporting became live. RF can see which employees or external workforce members can access sensitive information within folders or public chat channels in real time.

Remediation option was then applied to automatically remove permissions and content in areas of the organization where the risk of data leak is high. Users were nudged into reducing the sensitive files they shared over public channels or sharing via links for Google Drive.

The amount of time it took to get the full implementation up and running was much shorter than expected

"Installation took a minute"

## The Results

RF was fully protected against accidental or intentional data leaks from their core SaaS platforms. This protection was extended to shared channels over Slack Connect and Google Drive. Without any overhead in the day to day operations of RF and its external partners, 97% of all at-risk sensitive data is tracked and remediated appropriately in real time. Probably the most important value add from Polymer is to instill a culture of privacy & security within the workforce. The user warnings and activity tracking allows RF to design appropriate training programs to build a security culture.

"Look forward to trying out Zendesk and future Polymer Integrations"

With regular employee training, the email security team can also refine its rules. And they can separate legitimate messages from increasingly sophisticated attacks.

*Polymer protects against data loss (DLP) on modern collaboration tools like Slack, Dropbox, Zoom, Github and more with alerting & real-time redaction of sensitive and regulated information such as PII, PHI, financial and security data.*